UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,916	02/09/2004	Grigori M. Somin	30835/303181	1186

45373 7590 05/17/2007

MARSHALL, GERSTEIN & BORUN LLP (MICROSOFT)
233 SOUTH WACKER DRIVE
6300 SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	**PAPER NUMBER**
2109	

MAIL DATE	DELIVERY MODE
05/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,916	SOMIN ET AL.	
	Examiner	Art Unit	
	Benjamin A. Kaplan	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/9/2004 and 6/26/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-35 are non-statutory because the computer readable medium can be any medium and in the specification on page 7 lines 17-19 "Communications media typically embody computer-readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media." Specifically mentions a signal or carrier wave, which is non-statutory.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-35 are rejected under 35 U.S.C. 102(b) as being anticipated by Internet X.509 Public Key Infrastructure Certificate and CRL Profile. (RFC2459)

As Per Claim 1: RFC2459 teaches:

- A computer-readable medium containing an identity certificate data structure, the identity certificate data structure comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 "Because a certificate's signature and timeliness can be independently checked by a certificate-using client, certificates can be distributed via untrusted communications and server systems, and can be cached in unsecured storage in certificate-using systems.").
A X.509 certificate is this certificate. The certificate can be cached showing a computer readable medium.

- a first data field containing data representing an identity peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 "The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or on the issuer name and serial number.")
The Authority Key Identifier is the identity peer name as claimed.

- a second data field containing data representing an identity public key

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the

public key").

- the identity public key and an identity private key forming a public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 "The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.").

- a third data field containing data representing a certificate type, the certificate type indicating an identity certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 "An object identifier is defined for the private extension.").

- a fourth data field containing data representing a signature of the identity certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 "This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate.").

- the signature derived, at least in part from the identity private key.

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines "The authority key identifier extension provides a means of identifying the public key corresponding to the private

key used to sign a certificate.").

As Per Claim 2: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- the identity certificate data structure is an X.509 certificate

A X.509 certificate as seen in the rejection of claim 1 is inherently a X.509 certificate.

As Per Claim 3: The rejection of claim 2 is incorporated and further RFC2459 teaches:

- the first data field is a subject alternative name field of the X.509 certificate.

(Page 24 section 4.2.1.1 Authority Key Identifier first paragraph lines 3-7 "This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or on the issuer name and serial number.").

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 "The subject alternative names extension allows additional identities to be bound to the subject of the certificate.").

As Per Claim 4: The rejection of claim 2 is incorporated and further RFC2459 teaches:

- the third data filed is an extension property field of the X.509 certificate.

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 "An object identifier is defined for the private extension.").

As Per Claim 5: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- the identity peer name in the first data field is globally unique

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 "The value of the keyIdentifier field SHOULD be derived from the public key used to verify the certificate's signature or a method that generates unique values.").

As Per Claim 6: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- the identity peer name in the first data field is derived, at least in part, from the identity public key in the second data field

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5).

As Per Claim 7: The rejection of claim 6 is incorporated and further RFC2459 teaches:

- the identity peer name in the first data field is derived, at least in part, from a hash of the identity public key in the second data field

(Page 24 section 4.2.1.2 Subject Key Identifier paragraph 2 lines 4-7 "The value of the

subject key identifier MUST be **the value placed in the key identifier field of the Authority Key Identifier** extension (see sec. 4.2.1.1) of certificates issued by the subject of this certificate.").

(Section 4.2.1.2 Subject Key Identifier page 25 paragraph 2 "(1) The keyIdentifier is composed of the 160-bit SHA-1 **hash of** the value of the BIT STRING subject**PublicKey** (excluding the tag, length, and number of unused bits).").

As Per Claim 8: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- the identity private key is stored in a Cryptographic Service Provider container.

(Section 3.5 Management Protocols Page 13 subsection (d) lines 1-3 "key pair recovery: As an option, user client key materials (e.g., a user's private key used for encryption purposes) may be backed up by a CA or a key backup system.").

The key backup system is the Cryptographic Service Provider container, a backup is a form of storage.

As Per Claim 9: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- a fifth data field containing data representing an issuer of the identity certificate

(Page 17 section 4.1.2.4 Issuer lines 1-2 "The issuer field identifies the entity who has signed and issued the certificate.").

- a sixth data field containing data representing a subject of the identity certificate

(Page 21 section 4.1.2.6 Subject lines 1-2 "The subject field identifies the entity associated with the public key stored in the subject public key field.").

- wherein the issuer and the subject of the identity certificate are the same

(Page 21 section 4.1.2.6 Subject lines 3-8 "If the subject is a CA (e.g., the basic constraints extension, as discussed in 4.2.1.10, is present and the value of cA is TRUE,) then **the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field** (see sec. 4.1.2.4) in all certificates issued by the subject CA.").

As Per Claim 10: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- a fifth data field containing data representing a period of validity of the identity certificate.

(Page 20 section 4.1.2.5 Validity lines 1-3 "The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates:").

As Per Claim 11: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- a fifth data field containing data representing a version of the identity certificate

(Page 16 section 4.1.2.1 Version line 1 "This field describes the version of the encoded certificate.").

As Per Claim 12: RFC2459 teaches:

- A computer-readable medium containing a group root certificate data structure, the group root certificate data structure comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 as seen in the rejection of claim 1.).

(Page 9 section 3.2 Certification Paths and Trust paragraph 3 lines 1-3 "Internet Policy Registration Authority (IPRA): This authority, operated under the auspices of the Internet Society, acts as the root of the PEM certification hierarchy at level 1.").

A root X.509 certificate is this certificate. The certificate can be cached showing a computer readable medium.

- a first data field containing data representing a group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- a second data field containing data representing a group root public key

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- a third data field containing data representing a certificate type, the certificate type indicating a group root certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- a fourth data field containing data representing a signature of the group root certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

- the signature derived, at least in part from a group root private key.

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines as seen in the rejection of claim 1.).

- the group root private key and the group root public key in the second data field forming a public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

As Per Claim 13: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- the group root certificate data structure is an X.509 certificate

A X.509 certificate as seen in the rejection of claim 12 is inherently a X.509 certificate.

As Per Claim 14: The rejection of claim 13 is incorporated and further RFC2459 teaches:

- the first data field is a subject alternative name field of the X.509 certificate.

(Page 24 section 4.2.1.1 Authority Key Identifier first paragraph lines 3-7 as seen in the rejection of claim 3.).

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 as seen in the rejection of claim 3.).

As Per Claim 15: The rejection of claim 13 is incorporated and further RFC2459 teaches:

- the third data filed is an extension property field of the X.509 certificate.

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 4).

As Per Claim 16: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- the group peer name in the first data field is globally unique

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5.).

As Per Claim 17: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- the group peer name in the first data field is derived, at least in part, from the group root public key in the second data field

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5.).

As Per Claim 18: The rejection of claim 17 is incorporated and further RFC2459 teaches:

- the group peer name in the first data field is derived, at least in part, from a hash of the group root public key in the second data field

(Page 24 section 4.2.1.2 Subject Key Identifier paragraph 2 lines 4-7 as seen in the rejection of claim 7.).

(Section 4.2.1.2 Subject Key Identifier page 25 paragraph 2 as seen in the rejection of claim 7.).

As Per Claim 19: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- a fifth data field containing data representing an issuer of the group root certificate

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

- a sixth data field containing data representing a subject of the group root certificate

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

- wherein the issuer and the subject of the identity certificate are the same

(Page 21 section 4.1.2.6 Subject lines 3-8 as seen in the rejection of claim 9.).

As Per Claim 20: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- a fifth data field containing data representing a period of validity of the group root certificate.

(Page 20 section 4.1.2.5 Validity lines 1-3 as seen in the rejection of claim 10.).

As Per Claim 21: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- a fifth data field containing data representing a version of the group root certificate

(Page 16 section 4.1.2.1 Version line 1 as seen in the rejection of claim 11.).

As Per Claim 22: RFC2459 teaches:

- A computer-readable medium containing a group membership certificate data structure, the group membership certificate data structure comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 as seen in the rejection of claim 1.).

(Page 10 line 17-19 "CAs represent, for example, particular organizations, particular organizational units (e.g., departments, groups, sections), or particular geographical areas.")

A group level X.509 certificate is this certificate. The certificate can be cached showing a computer readable medium.

- a first data field containing data representing a group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- a second data field containing data representing an issuer peer name

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

- a third data field containing data representing a subject peer name

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

- a forth data field containing data representing a certificate type, the certificate type indicating a group membership certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- a fifth data field containing data representing a signature of the group membership certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

As Per Claim 23: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- the group membership certificate data structure is an X.509 certificate

A X.509 certificate as seen in the rejection of claim 22 is inherently a X.509 certificate.

As Per Claim 24: The rejection of claim 23 is incorporated and further RFC2459 teaches:

- the first data field is an extension property field of the X.509 certificate

(Page 24 section 4.2.1.1 Authority Key Identifier first paragraph lines 3-7 as seen in the rejection of claim 3.).

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 as seen in the rejection of claim 3.).

As Per Claim 25: The rejection of claim 23 is incorporated and further RFC2459 teaches:

- the second data field is an issuer alternative name field of the X.509 certificate

(Page 32 section 4.2.1.8 Issuer Alternative Names lines 1-3 "As with 4.2.1.7, this extension is used to associate Internet style identities with the certificate issuer. Issuer alternative names MUST be encoded as in 4.2.1.7.").

As Per Claim 26: The rejection of claim 23 is incorporated and further RFC2459 teaches:

- the third data field is a subject alternative name field of the X.509 certificate.

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 as seen in the rejection of claim 3.).

As Per Claim 27: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- the group peer name in the first data field is globally unique

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5.).

As Per Claim 28: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- the issuer peer name in the second data field is a reference to a certificate selected from the group consisting of: a group root certificate and a group membership certificate

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.)
It is inherent that since the issuer field identifies the entity that issued a certificate the issuing entity will be referred to in this field, as such any entity that can issue a certificate would be in the group of possible entries for this field.

As Per Claim 29: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- a sixth data field containing data representing a period of validity of the group membership certificate.

(Page 20 section 4.1.2.5 Validity lines 1-3 as seen in the rejection of claim 10.).

As Per Claim 30: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- a sixth data field containing data representing a version of the group membership certificate

(Page 16 section 4.1.2.1 Version line 1 as seen in the rejection of claim 11.).

As Per Claim 31: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- a sixth data field containing data representing a public key

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- the public key in the second data field forming a public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

As Per Claim 32: RFC2459 teaches:

- A computer-readable medium containing a group certificate chain data structure, the group certificate chain data structure comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 as seen in the rejection of claim 1.).

(Page 9 section 3.2 Certification Paths and Trust lines 7-8 "In general, a chain of multiple certificates may be needed,").

A X.509 certificate path or chain of certificates is this chain data structure. The certificates can be cached showing a computer readable medium.

- a first data field containing data representing a group root certificate, the group root certificate comprising

(Page 9 section 3.2 Certification Paths and Trust paragraph 3 lines 1-3 as seen in the rejection of claim 12).

(Document title X.509 Public Key Infrastructure Certificate and CRL Profile).

A root X.509 certificate is this certificate.

- a second data field containing data representing a group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- a third data field containing data representing a group root public key

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- a forth data field containing data representing a certificate type, the certificate type indicating a group root certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- a fifth data field containing data representing a signature of the group root certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

- the signature derived, at least in part, from a group root private key

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines as seen in the rejection of claim 1.).

- the group root private key and the group root public key in the third data field forming a public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

- a sixth data field containing data representing a group membership certificate the group membership certificate comprising

(Document title X.509 Public Key Infrastructure Certificate and CRL Profile)

(Page 10 line 17-19 as seen in the rejection of claim 22)

A group level X.509 certificate issued from the root certificate authority is this certificate.

- a seventh data field containing data representing a group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- the group peer name in the seventh data field being the same as the group peer in the second data field in the group root certificate

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 2 lines 1-3 "The keyIdentifier field of the authorityKeyIdentifier extension MUST be included in all certificates generated by conforming CAs to facilitate chain building.").

- an eighth data field containing data representing an issuer peer name

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

- the issuer peer name in the eighth data field being a reference to the group root certificate in the first data field

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).
It is inherent that since the issuer field identifies the entity that issued a certificate and the root certificate issued this certificate the root certificate would be referred to as the issuer.

- a ninth data field containing data representing a subject peer name

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

- a tenth data field containing data representing a certificate type, the certificate type indicating a group membership certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- an eleventh data field containing data representing a signature of the group membership certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

As Per Claim 33: The rejection of claim 32 is incorporated and further RFC2459 teaches:

- the group root certificate and the group membership certificate are X.509 certificates

X.509 certificates as seen in the rejection of claim 32 are inherently X.509 certificates.

As Per Claim 34: The rejection of claim 32 is incorporated and further RFC2459 teaches:

- a twelfth data field containing data representing a public key

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- the key and a private key forming a public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

As Per Claim 35: The rejection of claim 34 is incorporated and further RFC2459 teaches:

- a thirteenth data field containing data representing a second group membership

certificate, the second group membership certificate comprising:

(Document title X.509 Public Key Infrastructure Certificate and CRL Profile)

(Page 10 line 17-19 as seen in the rejection of claim 22)

A group level X.509 certificate issued from the group level X.509 certificate issued from the root certificate authority is this certificate.

- a fourteenth data field containing data representing a group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

- the group peer name in the fourteenth data field being the same as the group peer name in the second data field in the group root certificate

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 2 lines 1-3 as seen in the rejection of claim 32).

- a fifteenth data field containing data representing an issuer peer name

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

- the issuer peer name in the fifteenth data field being a reference to the group membership certificate in the sixth data field

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

It is inherent that since the issuer field identifies the entity that issued a certificate and

the certificate issued by the root certificate issued this certificate the first group membership certificate would be referred to as the issuer.

- a sixteenth data field containing data representing a subject peer name

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

- a seventeenth data field containing data representing a certificate type, the certificate type indicating a group membership certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- an eighteenth data field containing data representing a signature of the second group membership certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin A. Kaplan whose telephone number is 571-272-1395. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on 571-270-1392. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

Chameli C Das

CHAMELI DAS
SUPERVISORY PATENT EXAMINER

5/10/07